



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/575,568

04/11/2006

Dirk Gandolph

PD030108

1348

24498 7590 06/02/2010  
Robert D. Shedd, Patent Operations  
THOMSON Licensing LLC  
P.O. Box 5312  
Princeton, NJ 08543-5312

EXAMINER

POPHAM, JEFFREY D

ART UNIT

PAPER NUMBER

2437

MAIL DATE

DELIVERY MODE

06/02/2010

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/575,568	<b>Applicant(s)</b> GANDOLPH ET AL.	
	<b>Examiner</b> JEFFREY D. POPHAM	<b>Art Unit</b> 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 16 February 2010.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-4 and 18-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 18-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 April 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)                        | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Remarks***

Claims 1-4 and 18-32 are pending.

***Response to Arguments***

1. Applicant's arguments filed 2/16/2010 have been fully considered but they are not persuasive.

Applicant argues that "Kelly and/or Grooters fails to disclose or suggest at least the concept of the second data block that is specific to a specified group of removable storage media and that can be decrypted only if any storage medium of the specific group is accessible (e.g. in relation with some or all discs from a particular provider or studio)." It is noted that this is merely one example, and that a "group" is not defined in the independent claims as being any specific form of group. Therefore, under the broadest reasonable interpretation of a group (as in claim 1), a group contains 1 or more entities that are related in some fashion in such a manner that they are within the group. This could be the single medium that is currently being viewed, all media ever created, all media related to action films, all James Bond movies, etc. Any set of 1 or more media meet this limitation of the second data block being specific to a specified group. In Kelly, the supplemental data can only be decrypted when the storage medium is accessible, since the keys on the storage medium must be accessed in order to decrypt the supplemental data. Therefore, there is a group of media (which could be this 1 single medium, any of the other examples above, or a wide variety of other groups) that contains the keys that are required to decrypt the

Art Unit: 2437

supplemental data. When the medium is not accessible, the keys are not accessible and, therefore, the supplemental data cannot be decrypted.

With respect to Grooters, one may find teaching of a specified group of storage media in the channels and sub-channels used. As an example, a sub-channel for action movies has a sub-sub-channel for James Bond movies which have been previously viewed by the user. This creates groupings of content, in that action movies are grouped under the sub-channel for action and James Bond movies are grouped under the sub-sub-channel for James Bond movies. These channels store the supplemental information (albeit it does not appear to be stored on storage within the playback device, but it is stored within the user's network nonetheless) related to the topic for the channel. Therefore, the sub-sub-channel for James Bond movies will store supplemental information related to James Bond movies that the user has previously viewed. Therefore, when the user watches a James Bond DVD (at least those that have already been viewed), the user may access data within this sub-sub-channel related to such movies. Clearly, this is a group of media in that, upon accessing a James Bond DVD, the sub-sub-channel for such movies will be accessed such that the user may access the supplemental data related to James Bond movies.

Applicant goes on to argue that "Data retrieved from such title-related Internet search (or presumably rather, the link information retrieved from such title-related Internet search, as mentioned above) is added to appropriate sub-channels of a DVD channel. That means that no public data is stored, because the stored data is not public any more (as it is not Internet data)." If this is the

Art Unit: 2437

case, then the amendment to the claims, stating that the public data is stored within the playback device cannot occur. As Applicant is arguing that the data cannot be public since it is not "Internet data", then the claimed limitation of storing public data within the playback device is impossible. For purposes of prior art rejection, this has been construed as possible, since it is a claimed limitation and the Examiner sees no definition in the application that would limit the information stored on the playback device from being referred to as public data. However, Applicant's stance on this matter will have to be clarified such that the claims are clear.

Applicant also argues that "the combination teaches away from the present invention, in that such a combination actually teaches one skilled in the art to **limit access to additional content** .. In contrast, the present invention allows distribution and storage but limits only the decryption of additional content." Applicant then refers to various portions of the specification. It is noted, however, that the claims are not so limited as to this information provided in the specification. Furthermore, at least one embodiment of Kelly states that "It is also possible to distribute the additional content items 151 without any authentication, using the Disc Key or Title Key from the record carrier 101 as an encryption key to encrypt the additional content items 151 before distributing them" (Paragraph 64). Clearly, this teaches allowing distribution without authentication of the client, but limiting access by only allowing decryption to those devices that have an appropriate medium.

Art Unit: 2437

2. Applicant's arguments with respect to claims 1-4 and 18-32 with respect to the first storage medium being within the playback device have been considered but are moot in view of the new ground(s) of rejection.

### ***Specification***

3. The disclosure is objected to because of the following informalities: The third paragraph on page 4 states "This method is disclosed in claim 1. An apparatus that utilizes the method is disclosed in claim 6." It is noted that claim numberings change throughout prosecution and, even now in the instant application, claim 6 has been cancelled, such that this reference to claim 6 in the specification is meaningless. Furthermore, the limitations of each claim may be amended and/or the numbering of each claim may change further as claim renumbering will be required due to the cancelled claims and any further cancelled claims. Applicant is therefore reminded of their duty to provide a clear disclosure and is hereby put on notice that Applicant must amend the specification during prosecution to reflect any changes to the subject matter disclosed by reference to a claim number. Alternatively, Applicant may amend the specification such that the subject matter of the referenced claim is in the text of the specification. All amendments or claims must find descriptive basis in the original disclosure or they involve new matter. No new matter may be added. See MPEP §§ 608, 608.01, 608.01(g), 608.01(o).

Appropriate correction is required.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 3, 18, 20, 22, 23, 25, 26, and 28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly (U.S. Patent Application Publication 2003/0072453) in view of Grooters (U.S. Patent 6,931,593) and Piotrowski (U.S. Patent Application Publication 2002/0188959).

Regarding Claim 1,

Kelly discloses a method for decrypting data within a playback device, the data comprising an encrypted first data set being audiovisual presentation data and an encrypted second data set being audiovisual supplementary data relating to the first data set, wherein the first data set and at least two corresponding device independent electronic decryption keys are stored in a first removable prerecorded medium (Abstract; and Paragraphs 29, 31-34, 51, and 63-64; disc keys and title keys stored on the medium along with a movie or other audiovisual content, for example), and the second data set is not stored on the first removable prerecorded storage medium but on a second storage medium and is related to the first data set (Abstract; and Paragraph 30;

Art Unit: 2437

additional content items from the server that are related to the content on the disc, for example), the second storage medium having a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the first of removable prerecorded storage medium (Paragraphs 4, 12, 30, and 31; additional content items including interviews with actors and other participants, live events, and online games related to the movie comprising, for example, group content; and additional scenes, different endings, different soundtracks, etc. comprising, for example, content specific to the medium), the method comprising the steps of:

Retrieving the first data set and the device independent decryption keys from the first removable storage medium (Abstract; and Paragraphs 34-36; retrieving the content or encrypted titles and the keys from the disc, for example);

Retrieving the second data set from the second data block of the second storage medium (Abstract; and Paragraphs 50 and 57; downloading additional content items from the server, for example);

Decrypting the first data set using a first of the decryption keys (Abstract; and Paragraphs 36 and 44; decrypting the encrypted titles, for example); and

Decrypting the second data set using a second of the decryption keys that is different from the first of the decryption keys



(Abstract; and Paragraphs 50-52, 58-59, and 63-64; as an example, paragraph 63 discusses using the encrypted Disc key as the session key that is used to encrypt additional content items from the server. This Disc key is not actually used to decrypt the content itself (the title keys are used to decrypt the content while the Disc key is used to decrypt the title keys). Therefore, the encrypted Disc key being used to decrypt additional content is different from the first key which was used to decrypt the first data set (encrypted title). In another interpretation, a title key that is not being currently used to decrypt content on the disk may be used in the decryption of the additional content, and this would correspond to a different key being used, for example).

But does not appear to explicitly disclose that the second storage medium has a first data block that is public or that the second storage medium is within the playback device.

Grooters, however, discloses the second storage medium having a first data block that is public, a second data block that is specific to a specified group of removable storage media and a third data block that is specific to the removable prerecorded storage medium (Column 5, line 61 to Column 6, line 25; Column 7, line 47 to Column 8, line 18; and Column 8, lines 47-52; additional content is retrieved from the Internet that all may access (public), such as content regarding shopping, sports, business, etc. from

Art Unit: 2437

publicly-accessible websites, such as ESPN.com or concert schedules for a particular band; further additional content is related to a particular movie or song, for example based on a DVD or CD that is inserted in the client; and yet further additional content is related to a group of media, such as by providing information related to action movies or James Bond movies, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the information accessing techniques of Grooters into the secure content distribution system of Kelly in order to allow the system to acquire further additional content in a wide variety of manners (e.g. sub-channels, sub-sub-channels, Internet searching, local network searching, etc.), thereby allowing each user to access additional content that is desirable by that user.

Piotrowski, however, discloses that the second storage medium is within the playback device (Paragraph 44; supplemental multimedia information being provided to the computer via a memory storage device, which would be within the playback device, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the supplemental data distribution techniques of Piotrowski into the secure content distribution system of Kelly as modified by Grooters in order to allow the system to distribute the supplemental

Art Unit: 2437

information in multiple fashions, such as over the Internet in order to provide the most up-to-date supplemental information, as well as via a storage medium in order to allow devices to access supplemental information while they are offline and not connected to the Internet, thereby allowing the system to reach additional users (e.g. users without an Internet connection whatsoever or users that are using a DVD player that is not connected, as examples).

Regarding Claim 18,

Claim 18 is an apparatus claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 1, in addition, Kelly discloses detecting whether the first removable storage medium and the second data set are authorized by the same authority, wherein the second data set is regarded as authorized if it can be decrypted by the second decryption key (Abstract; and Paragraphs 50-52, 58-59, and 63-64).

Regarding Claim 22,

Claim 22 is an apparatus claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 20,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 1, in addition, Kelly discloses that the first electronic decryption key is the only suitable key for decrypting the first data set, and the second decryption key is one of several suitable keys for decrypting the second data set (Abstract; and Paragraphs 36, 44, 51, 58-59, and 63-64; the title keys may be used to decrypt the first data set on the medium, but various keys are able to decrypt the additional content, for example).

Regarding Claim 23,

Claim 23 is an apparatus claim that corresponds to method claim 20 and is rejected for the same reasons.

Regarding Claim 26,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 1, in addition, Kelly discloses retrieving a third data set from the third data block and decrypting the third data set using the second of the decryption keys (Abstract; and Paragraphs 4, 12, 30, 31, 50-52, 58-59, and 63-64).

Regarding Claim 28,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 1, in addition, Kelly discloses that the specified group of removable storage media comprises only media that are provided by a particular provider (Paragraphs 4, 12, 30, and 31; in order to access the additional content, a user must own a legitimate

Art Unit: 2437

specimen of the disc, meaning that the disc must be a properly produced medium from the provider that creates and/or distributes that particular disc). Grooters also discloses that the specified group of removable storage media comprises media that are provided by a particular provider (Column 7, lines 10-59; providing channels related to a recording label, which would correlate to a provider, and extend to movie studios that produce a movie on the disk, for example).

Regarding Claim 25,

Claim 25 is an apparatus claim that corresponds to method claim 28 and is rejected for the same reasons.

Regarding Claim 29,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 1, in addition, Kelly discloses that the second data block of the second data set can only be decrypted if any one of the specified group of removable storage media is accessible (Abstract; and Paragraphs 36, 44, 51, 58-59, and 63-64; the data cannot be accessed unless the keys are accessible via a proper medium, for example).

Regarding Claim 31,

Claim 31 is an apparatus claim that corresponds to method claim 29 and is rejected for the same reasons.

Regarding Claim 30,

Kelly as modified by Grooters and Piotrowski discloses the method of claim 29, in addition, Kelly discloses that the specified group of removable storage media is a predefined group that is provided by the same provider as the first removable storage medium (Paragraphs 4, 12, 30, and 31); and Grooters discloses that the specified group of removable storage media is a predefined group that is provided by the same provider as the first removable storage medium (Column 7, lines 10-59).

Regarding Claim 32,

Claim 32 is an apparatus claim that corresponds to method claim 30 and is rejected for the same reasons.

5. Claims 2 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Grooters and Piotrowski, further in view of Getsin (U.S. Patent 6,529,949).

Regarding Claim 2,

Kelly as modified by Grooters and Piotrowski does not explicitly disclose determining from a plurality of data sets on the second storage medium a second data set that refers to the first removable storage medium, wherein the data sets refer to different removable prerecorded storage media.

Getsin, however, discloses determining from a plurality of data sets on the second storage medium a second data set that

Art Unit: 2437

refers to the first removable storage medium, wherein the data sets refer to different removable prerecorded storage media (Column 27, line 56 to Column 29, line 4; showing different content being provided based on the medium that is currently being played, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote playback control system of Getsin into the secure content distribution system of Kelly as modified by Grooters and Piotrowski in order to provide supplemental data for a plurality of media (e.g. DVDs), allowing clients to access the data directed to the media for which the client currently has access (such as the content being played), while ensuring authentication and authorization of the user, client, and/or DVD before allowing access to such supplemental data, and/or to allow the system to access supplemental data held on the currently playing DVD via such authentication and authorization processing.

Regarding Claim 19,

Claim 19 is an apparatus claim that corresponds to method claim 2 and is rejected for the same reasons.

6. Claims 4, 24, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Grooters and Piotrowski, further in view of Qawami (U.S. Patent Application Publication 2002/0176575).

Regarding Claim 4,

Kelly as modified by Grooters and Piotrowski does not explicitly disclose that the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains the electronic decryption keys is readable.

Qawami, however, discloses that the electronic decryption keys are only accessible while a removable prerecorded storage medium that contains the electronic decryption keys is readable (Paragraphs 38, 42, 44, 54-58, and 94; the media key is never retained within the device, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key/content protection techniques of Qawami into the secure content distribution system of Kelly as modified by Grooters and Piotrowski in order to only provide access to keys while the keys are being used to decrypt specific data on the disk, and to delete the keys immediately after use, thereby only storing keys for the amount of time it takes to decrypt the data, and/or to only provide access to decrypted content in portions that are rewritten as soon as they are rendered, thereby increasing security of the keys as well as the content.

Regarding Claim 27,



Kelly as modified by Grooters and Piotrowski does not explicitly disclose that the encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered.

Qawami, however, discloses that the encrypted data are stored within the player, and wherein decrypted data are only temporarily buffered (Paragraph 55; temporarily storing only currently required portions of decrypted data, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the key/content protection techniques of Qawami into the secure content distribution system of Kelly as modified by Grooters and Piotrowski in order to only provide access to keys while the keys are being used to decrypt specific data on the disk, and to delete the keys immediately after use, thereby only storing keys for the amount of time it takes to decrypt the data, and/or to only provide access to decrypted content in portions that are rewritten as soon as they are rendered, thereby increasing security of the keys as well as the content.

Regarding Claim 24,

Claim 24 is an apparatus claim that corresponds to method claim 27 and is rejected for the same reasons.

Art Unit: 2437

7. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of Grooters and Piotrowski, further in view of Schneier (Schneier, Bruce, "Applied Cryptography", Second Edition, 1996, pp. 1-14).

Kelly as modified by Grooters and Piotrowski does not explicitly disclose that the first and second data sets are encrypted using RSA coding.

Schneier, however, discloses that the first and second data sets are encrypted using RSA coding (Pages 6-14). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the encryption algorithm of Schneier into the secure content distribution system of Kelly as modified by Grooters and Piotrowski in order to use an encryption algorithm that is well known, easy to understand and implement, widely used, and secure.

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory

Art Unit: 2437

period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2437

Jeffrey D Popham  
Examiner  
Art Unit 2437

/Jeffrey D Popham/  
Examiner, Art Unit 2437